Information Security Risk Analysis SWOT

Halyna Shevchenko[a], Svitlana Shevchenko[b], Yuliia Zhdanova[b], Svitlana Spasiteleva[b], and Olena Negodenko[a]

[a] *State University of Telecommunications, 7 Solomyanska str., Kyiv, 03110, Ukraine*
[b] *Borys Grinchenko Kyiv University, 18/2 Bulvarno-Kudriavska str., Kyiv, 04053, Ukraine*

Abstract

The rapid growth of digital information and its increasing importance creates the preconditions for the emergence of new information security risks: leakage, theft, loss, distortion, forgery, destruction, copying and blocking of information, and, consequently, harm to the organization. Therefore, information risks take one of the central places in the risk theory. The approach of assessment and management of information risks is now used as a systematic methodology for information protection. This paper proposes an approach to information risk analysis, namely: the introduction of SWOT-analysis tools for identification and assessment of risks in the field of small and medium-sized businesses informational security. Based on scientific sources, the main definitions of the study are analyzed: information security risk, quantitative risk assessment (qualitative and quantitative approach), SWOT-analysis technology. The content and procedure of SWOT analysis are described. Emphasis is placed on developing and identifying aspects such as internal weaknesses of the organization and external threats in order to counter threats to information security (violation of confidentiality, accessibility, and integrity), as well as the use of external opportunities for its development. The choice of this technology is most reasonable for those enterprises with a small presence of specialists in this field.

Keywords

Information security (IS) risks, IS risk assessment, SWOT-analysis, assets, threats, vulnerabilities.

1. Introduction

For the first time ever, Cyber incidents (39% of responses) rank as the most important business risk globally in the [1]. This is obvious because according to the study [2], losses resulting from external incidents, such as DDoS attacks or phishing and malware/ransomware campaigns, account for the majority of the value of claims analyzed (85%), followed by malicious internal actions (9%) which are infrequent but can be costly. Accidental internal incidents, such as employee errors while undertaking daily responsibilities, IT or platform outages, systems, and software migration problems or loss of data account for over half of cyber claims analyzed by number (54%). All this indicates that any technical failures of equipment or inattention of personnel, or the implementation of external threats makes impossible access to data or leads to their loss (violated the availability, integrity, and confidentiality of the information). As a result, the organization suffers great losses or goes bankrupt. Especially these days the Covid-19 pandemic has made adjustments to the work of companies and employees mostly work remotely, creating the preconditions for the growth of cyber incidents. Therefore, the problem of information security is a priority and needs constant improvement.

Cybersecurity Providing in Information and Telecommunication Systems, January 28, 2021, Kyiv, Ukraine
EMAIL: foxik.ryzyy@gmail.com (A.1); s.shevchenko@kubg.edu.ua (B.2); y.zhdanova@kubg.edu.ua (B.3); s.spasitielieva@kubg.edu.ua (B.4); negodenkoav@i.ua (A.5)
ORCID: 0000-0002-8717-4358 (A.1); 0000-0002-9736-8623 (B.2); 0000-0002-9277-4972 (B.3); 0000-0003-4993-6355 (B.4); 0000-0001-6645-1566 (A.5)


Recently, the approach to assessing and managing information risks in order to ensure the organization's information security has been used as a systematic methodology for information protection. The analysis of scientific sources allowed us to distinguish different approaches to risk management in the field of information security. Including:

- Risk-oriented approach to information security management of the enterprise [3].
- Risk assessment algorithms based on international standards and methods [4–6].
- Mathematical models based on fuzzy sets and fuzzy logic [7], based on the attack tree [8].
- Algorithms based on the comparison of different methods of IS risk management [9], a comprehensive structure of IS risk management, which includes the integration of the cascade effect of interconnected components of SPS (Cyber-Physical System) taking into account vulnerabilities, threats, and risks to assets [10].

Our study proposes a technology for qualitative risk analysis of information security (IS), namely: SWOT-analysis tools for risk assessment in the field of IS of small and medium-sized businesses in order to develop a strategy for countering external threats, while identifying its internal weaknesses.

2. SWOT Analysis

Most small and medium-sized enterprises face a number of problematic issues in the field of IS risk management. In particular:

1. Impossibility of early identification of IS risk.
2. Lack of analytical department in this area; most often in the organization one person is responsible for information security, which, of course, will not use complex modeling methods (for example, the Monte Carlo method) or use complex algorithms for calculating risk.
3. Lack of criteria for assessing the risks of IS in the organization, on the basis of which a comparative analysis with the received estimates for further risk processing.
4. Lack of IS risk processing and response plans.
5. The imperfection of the system for discussing and disseminating information about the threats and vulnerabilities that characterize most companies.
6. High cost of international methods of IS risk management, which makes it impossible to implement them in small enterprises.

SWOT analysis is the initial stage of planning the strategy of the organization, can serve as a starting point for a more detailed study of problems in the field of IS risks, is quite easy to use, and does not require experienced experts to conduct it.

The above confirms the relevance of our study.

3. SWOT Analysis Technology

3.1. Historical Background

The authors of the research [11], [12] claim that there is no documented history of SWOT analysis. The historical development of SWOT analysis is presented in [11]. SWOT is credited to two Harvard Business School Policy Unit professors—George Albert Smith Jr and C Roland Christiensen during the early 1950s. Later in the 1950s another HBS Policy Unit professor Kenneth Andrews developed its usage and application. All professors were specialists in organizational strategy as opposed to marketing. SWOT went on to be developed by the HBS during the 1960s until SWOT became the tool that we use today.

Wheelan and Hunger (1998) used SWOT to look for gaps and matches between competencies and resources and the business environment. Dealtry (1992) considered SWOT in terms of groups and vectors with common themes and interactions. Shinno et al (2006) amalgamated SWOT-analysis with an Analytic Hierarchy Process (AHP) which ranked and prioritized each element using the software.

3.2. SWOT Analysis Matrix and its Components

Analysis SWOT research procedure, the idea of which is a comprehensive description of strengths (Strength), weaknesses (Weakness), opportunities (Opportunities), threats (Threats) in the development of organizational strategy. The content of this procedure is as follows:

1. The forces are studied—the competitive advantages of the organization in certain areas.
2. Weaknesses are studied—negative internal factors.
3. Political, economic, technological, social factors of the organization's macroenvironment are studied in order to identify strategic and tactical threats and timely prevent losses from them.
4. The strategic and tactical capabilities of the organization necessary to reduce "weaknesses" and strengthen "forces" are studied.
5. The forces agree with the possibilities for the formation of a new strategy [13, p.107].

This technology is made out in the form of a matrix which is presented in Table 1, and the decision in Table 2.

Table 1.
SWOT analysis

Strength	Weakness
S1.	W1.
S2.	W2.

Opportunities	Threats
O1.	T1.
O2.	T2.
O3.	T3.

Table 2.
SWOT-matrix of strategic decisions

	Threats (T)	Opportunities (O)
Strength (S)	Maximize strengths to counter ST threats	Maximize strengths to take advantage of the SO environment
Weakness (W)	Minimize the impact of weaknesses and avoid the threat of WT	Minimize the impact of weaknesses due to the capabilities of the external environment WO

4. Information Security Risks and Related Concepts

To use SWOT-analysis technology in IS risk management, it is necessary to introduce some definitions that appear in this study.

The authors [14] based on the analysis of scientific sources identified key points related to the concept of IS risk:

1. There is no unambiguous interpretation of the concept of "IS risk."
2. Identify the concepts of "information risk" and "information security risk."
3. "IS risk" is used only when there is a possibility of negative consequences.
4. "IS risk" is considered as a combination of the probability of the event and its consequences.
5. The concept of "IS risk" is a combination that combines other key terms (assets, vulnerabilities, threats, damage).

Taking into account all these factors, we consider the information security risk as a potential threat posed by the use of asset vulnerabilities to harm the organization and can be expressed by a numerical

and/or verbal function that describes the likelihood of IS threats and the amount of damage from their implementation.

An asset is a resource that represents value to an organization. Among the assets are information – tangible or intangible object, which:

- Is information or contains information.
- Has to value for the organization.

Vulnerability intrinsic properties of something resulting in susceptibility to a risk source that can lead to an event with a consequence [15].

IS threat – a possible cause of an undesirable incident that may damage the properties of IS: confidentiality, availability, the integrity of information (information assets) of the organization.

In order for a threat to become a real attack, it is necessary for the source of the IS threat (subject, material object, physical phenomenon) to be activated.

Under the management of IS risks (risk management) means a continuous cyclical process, which includes the following stages: risk identification (collection of information on assets, sources of threats, classification of threats and vulnerabilities; risk ranking); risk analysis (qualitative and quantitative approach to risk assessment); risk assessment (the process of comparing the quantified risk with these risk criteria to determine the significance of IS risk); risk processing and acceptance. Figure 1 shows the algorithm of the IS risk management process [16].

Implementing this algorithm, we consider the risk management of IS based on SWOT-analysis, focusing on confronting the internal weaknesses of the organization to external threats and building the strategy of the organization, using its strengths and external capabilities.

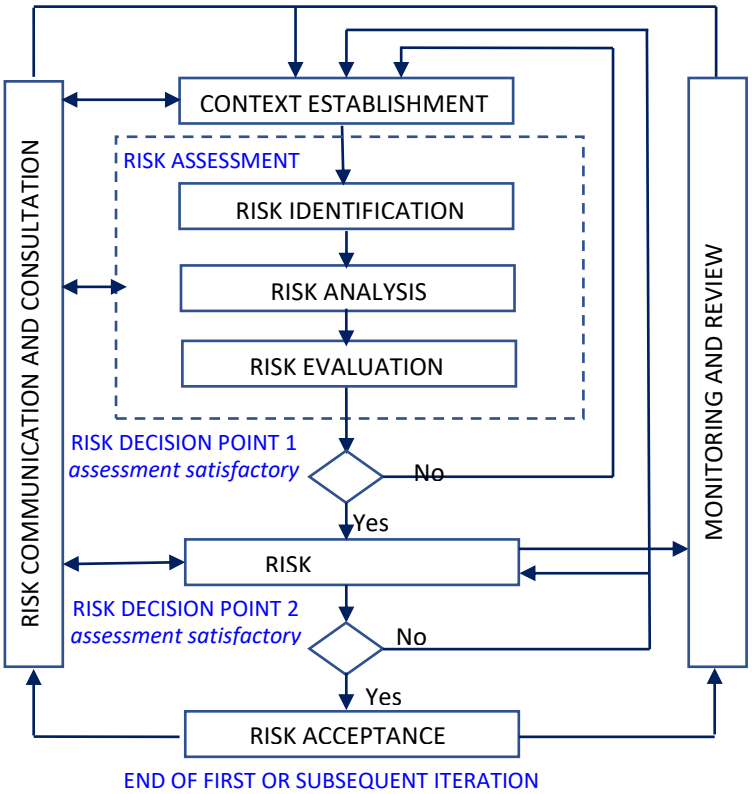

Figure 1: Illustration of an information security risk management process

5. SWOT Analysis of IS Risks

One of the disadvantages of SWOT analysis is the lack of comparability with competing companies [12], but in the risk management of companies IS this function is not a priority, which confirms the feasibility of its implementation.

IS risk management depends significantly on the collection of information about the asset to be protected, its vulnerabilities, threats, and their sources, as well as how objectively the relevant risk will be assessed based on the information provided.

Consider two options for SWOT-analysis of IS risks: qualitative SWOT-analysis and quantitative SWOT-analysis. A qualitative approach to quantifying IS risks uses a verbal scale of possible consequences (low, medium, and high) and the probability of these consequences. Advantages: intelligibility to all staff; Disadvantages: the subjectivity of this choice. This approach is used:

- As a starting point in identifying the risks of IS, which will be further analyzed in more detail.
- If such an analysis is sufficient to make a decision.
- If numerical data or resources are not sufficient for quantification.

The quantitative approach to quantifying IS risks uses a scale with numerical values for both consequences and probabilities, based on data obtained from different sources. Advantages: direct connection with the tasks and needs of the organization in IS, as it uses the actual data for the previous period about IS incidents; Disadvantages: Lack of data on new IS risks and vulnerabilities [14].

5.1. Qualitative SWOT Analysis of IS Risks

After collecting information about the information asset that needs protection, it is necessary to fill in Table 1. Based on it, create Table 2. An example is shown in Tables 3 and 4.

Table 3.
SWOT-analysis of IS risks

Strength	Weakness
S1. The most valuable assets have new hardware and software information security	W1. Insufficient information protection system for employees who work remotely
S2. Certified means of information protection	W2. Lack of a regular backup system
S3. Two-factor authentication is available	W3. Difficulties in the modernization of IT technologies
Opportunities	**Threats**
O1. IS risk insurance	T1. Natural disasters
O2. Establishing interaction with business partners, investors	T2. Attracting competitors to the best IB staff
O3. Outsourcing	T3. Fraudulent intrusion (hackers, computer criminals, fired employees)

Table 4
SWOT-matrix of strategic decisions

	Threats (T)	Opportunities (O)
Strength (S)	S1T3. Carrying out constant monitoring	S3O2. Transfer of part of the business
Weakness (W)	W3T2. Investments to improve IT technologies	W1O1. Differentiation of access rights

Since our study focuses on the interaction of weaknesses (asset vulnerabilities) and external threats, the SWOT matrix of strategic decisions can be represented by an interactive matrix. For example, Table 5.

Table 5
The interactive ranking matrix between external threats and internal weaknesses of the organization

	T1	T2	T3
W1	+	+	+
W2	+	0	+
W3	0	+	+

The priority is the threat that has the most combinations with the weaknesses of the organization (in our example it is T3).

5.2. Quantitative SWOT Analysis of IS Risks

The qualitative result of the SWOT analysis is considered by most scientists to be superficial, which subjectively and insufficiently provides an analysis of external and internal factors. It is obvious to support this analysis with quantitative estimates. To do this, we use a combination of the method of hierarchy analysis (AHP) with SWOT technology [17–20].

This process is shown in Figure 2.

We will describe each step.

Step 0. Select the asset that needs protection.

Step 1. Determine the context of IS risks in the organization. To do this, identify and compile a list of vulnerabilities of this asset and a list of threats. In our study, we focus on the weaknesses of the organization and external threats.

Step 2. Collect statistics. For example, the number of incidents in which threats exploited the vulnerability of an asset.

Step 3. Determine the weights to assess vulnerabilities and external threats. To do this, we will use the same coefficients for both external and internal factors. We use the method of hierarchies (AHP), proposed by T. Saati [18, 19].

Step 4. Calculate the degree of risk by the formula $r_{ij} = p_i \cdot q_j$, here p_i is the degree of vulnerability of the resource to the threat, q_j is the realization of the threat probability estimation.

Step 5. Create an interactive matrix with two inputs: rows—vulnerabilities W_i, columns—threats T_j, and at their intersection—r_{ij}.

Step 6. Calculation of the total risk degree $R_{\text{empirical}} = \sum r_{ij}$ for this asset.

Step 7. Compare the empirical risk degree with the critical one, which is defined in the organization. If $R_{empirical} < R_{critical}$, then go to Step 8; if $R_{empirical} \geq R_{critical}$, then go to Step 9.

Step 8. Accept the risk of IS and build an organizational strategy.

Step 9. Process the empirical degree of risk and calculate $R_{residual}$.

Step 10. Compare the residual degree of risk with the critical. If $R_{residual} < R_{critical}$, then go to Step 8; if $R_{residual} \geq R_{critical}$, then go to Step 2 to gather additional information.

Next, it is necessary to determine the overall risk degree for each asset that is valuable to the organization and needs protection. Arrange these risks, document and periodically monitor them.

Based on the algorithm, Python software was developed, today it is being tested and improved.

The qualitative and quantitative SWOT analysis was introduced into the educational process of 3rd-year students majoring in 125 Cybersecurity at Borys Grinchenko Kyiv University in the course of the discipline “Risk Theory.”

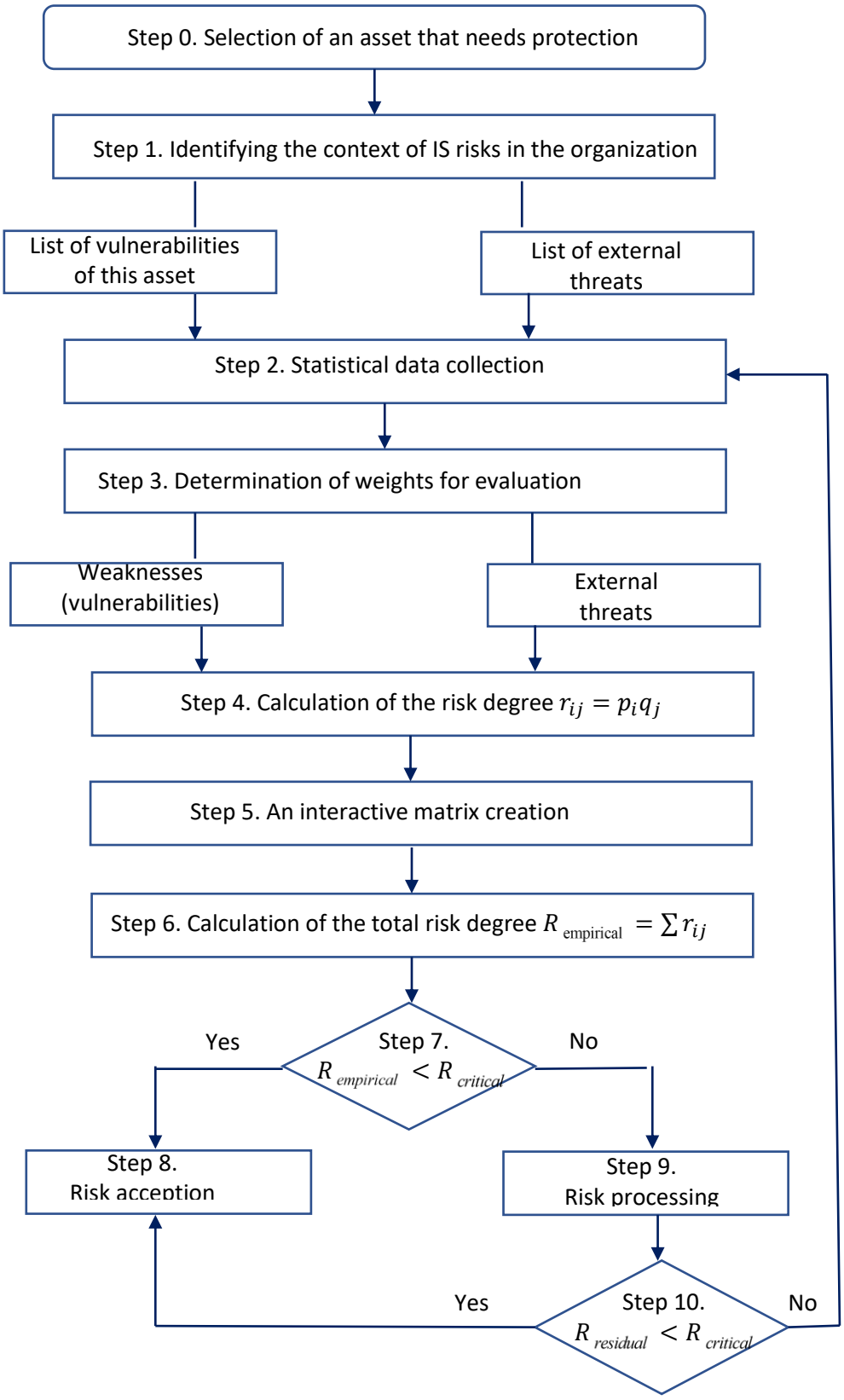

Figure 2: Algorithm for quantitative SWOT-analysis of IS risks

6. References

[1] Allianz Risk Barometer, Global risks, Report, January 2020. URL: https://www.agcs.allianz.com/news-and-insights/reports/allianz-risk-barometer.html

[2] Allianz: Cyber crime brings expensive losses for companies, but internal failures most frequent cause of cyber claims, Press release, November 19, 2020. URL: https://www.agcs.allianz.com/news-and-insights/news/cyber-risk-trends-2020.html

[3] T. V. Savelieva, O. M. Panasco, O. M. Prigodyuk, Analysis of methods and tools for implementing a risk-oriented approach in the context of information security of the enterprise, Bulletin of Cherkasy State Technological University 1 (2018) 81–89. doi: 10.24025/2306-4412.1.2018.153279Yu. R. Garasym, V. A. Romaka, M. M. Rybiy, Analysis of the process of information security risk management in the process of ensuring the survivability of systems, Bulletin of the National University "Lviv Polytechnic" 753 (2013) 90–99. URL: http://nbuv.gov.ua/UJRN/VNULP_2013_753_17.

[4] S. Dashti, P. Giorgini, E. Paja, Dashti, S., Giorgini, P., Paja, E.: Information Security Risk Management, in: The Practice of Enterprise Modeling, Springer International Publishing, Cham, 2017, pp. 18–33. doi: 10.1007/978-3-319-70241-4_2.

[5] D. Macek, I. Magdalenic, N. Ivkovic. Information Security Risk Assessment in Financial Institutions Using VECTOR Matrix and OCTAVE Methods – ProQuest, in: Proceedings of the 22nd Central European Conference on Information and Intelligent Systems, 2011, pp. 133-138. https://search.proquest.com/openview/d09aad9fb4846670b6c15c1ec3646bdd/1?pq-origsite=gscholar&cbl=1986354

[6] G. Melnyk, Model of information risk assessment in corporate systems, Bulletin of Kyiv National University named after Taras Shevchenko 6 (2015) 48–54. URL: http://www.library.univ.kiev.ua/ukr/host/10.23.10.100/db/ftp/visnyk/ekonom_171_2015.pdf

[7] B. Karabey, N. Baykal, Attack tree based information security risk assessment method integrating enterprise objectives with vulnerabilities, Int. Arab J. Inf. Technol. 10 (2013) 297–304. URL: https://www.semanticscholar.org/paper/Attack-tree-based-information-security-risk-method-Karabey-Baykal/bb1dee28dcf724747e789b762b04cd8513a8df26#references

[8] S. Fenz, J. Heurix, T. Neubauer, F. Pechstein, Current challenges in information security risk management, Information Management & Computer Security 22 (2014) 410–430. doi:10.1108/IMCS-07-2013-0053

[9] H. I. Kure, S. Islam, M. A. Razzaque. An Integrated Cyber Security Risk Management Approach for a Cyber-Physical System, Applied Sciences 8 (2018). URL: https://www.mdpi.com/2076-3417/8/6/898#cite

[10] T. Friesner, History of SWOT Analysis, 2011. URL: https://www.marketingteacher.com/history-of-swot-analysis/

[11] E. Gurel, SWOT analysis: a theoretical review, Journal of International Social Research 10 (2017) 994–1006. doi:10.17719/jisr.2017.1832

[12] Dictionary of systems analysis in public administration. K., 2006. URL: http://academy.gov.ua/NMKD/library_nadu/Encycloped_vydanniy/f4a14404-2b5a-4031-968c-c95c5a50b4c5.pdf

[13] S. M. Shevchenko, Yu. D. Zhdanova, S. O. Spasiteleva, P. M. Skladannyi, Conducting a SWOT-analysis of information risk assessment as a means of formation of practical skills of students specialty 125 cyber security, Cybersecurity: education, science, technology 2 (2020) 158–168. doi:10.28925/2663-4023.2020.10.158168.

[14] ISO GUIDE 73:2009(E/F), Risk management — Vocabulary, 2009, URL: https://www.iso.org/ru/standard/44651.html

[15] DSTU ISO/IEC 27005:2019 (ISO/IEC 27005:2018, IDT) "Information technology — Security techniques — Information security risk management," 2019. URL: http://online.budstandart.com/ru/catalog/doc-page.html?id_doc=85797

[16] H.-H. Chang, W. Chih, Application of a quantification SWOT analytical method, Mathematical and Computer Modelling 43 (2006) 158–169 https://doi.org/10.1016/j.mcm.2005.08.016.

[17] T. L. Saaty, L. G. Vargas, Models, Methods, Concepts & Applications of the Analytic Hierarchy Process. Kluwer Academic Publishers, Boston,1990.
[18] T. L. Saaty, The Analytic Hierarchy Process. McGraw-Hill, New York, 1980.
[19] A. M. Golitsyn, I. P. Repnikova, Using the method of analysis of hierarchies in SWOT-diagnostics of the marketing environment of the enterprise on the example of the Ukrainian manufacturer of anti-virus software, Eastern Europe: economy, business and management 20 (2019) URI: http://srd.pgasa.dp.ua:8080/xmlui/handle/123456789/2204